IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

UNITED STATES OF AMERICA v. OLDEN ELLERBE, III, *Defendant*.	Case No. 3:24CR009 18 U.S.C. § 1349 Conspiracy to Commit Bank Fraud (Count 1) 18 U.S.C. § 1708 Possession of Stolen Mail (Count 2) Forfeiture Allegation

CRIMINAL INFORMATION

THE UNITED STATES ATTORNEY CHARGES THAT:

COUNT ONE

(Conspiracy to Commit Bank Fraud)

From in or about January 2023, through in or about November 2023, the exact dates being unknown, in the Eastern District of Virginia and elsewhere, the defendant, OLDEN ELLERBE, III ("ELLERBE"), knowingly and intentionally combined, conspired, confederated, and agreed with others known and unknown to commit an offense contained with Chapter 63 of Title 18 of the United States Code, to wit: Bank fraud, that is, to knowingly execute and attempt to execute a scheme and artifice to defraud and to obtain money, funds, credits, assets, and securities owned by and under the custody and control of a financial institution as defined under Title 18, United States Code, Section 20, by means of materially false and fraudulent pretenses, representations, and promises, in violation of Title 18, United States, Code, Section 1344.

Object of the Scheme and Artifice to Defraud

The object of the scheme and artifice to defraud was for ELLERBE and his co-conspirators to fraudulently obtain funds to which they were not entitled through a number of illicit means, to include negotiating counterfeit and fraudulent checks at banks and utilizing stolen access devices to withdraw United States currency.

The Ways, Manner, and Means of the Conspiracy

The ways, manner, and means by which ELLERBE and his co-conspirators sought to accomplish the conspiracy operated in substance as follows:

1. Conspirators stole or otherwise unlawfully obtained United States Mail through a variety of means, to include the use of stolen or otherwise misappropriated United States Postal Service "Arrow" keys, which unlock all Postal Service blue collection boxes within a given geographic area. Blue collection boxes often contain mailings that consist of personal and business checks, United States currency, money orders, financial institution access devices (such as credit and debit cards), and other personally identifiable information.

2. Conspirators would then repurpose stolen checks—either through creating new check templates that incorporated the personal and financial information contained on the original check (to include the payor's name and address, as well as the account number and routing number), or replacing the name of the designated payee on the original check with the name of a conspirator or accomplice.

3. Conspirators would then obtain funds from financial institutions via the negotiation of these fraudulent checks through a number of means. One of those means was a practice known colloquially as "card-cracking," a four-prong process that typically proceeds as follows:

a. conspirators obtain the bank account information of a frequently complicit third

party (to include that bank account holder's Automated Teller Machine (ATM) card and accompanying Personal Identification Number (PIN)), usually on the understanding that the account holder will receive a future cash payment in exchange for these materials;

b. conspirators obtain the personal information and bank account information of a victim (to include the victim's bank account number and routing number) – typically through direct mail theft, or the purchase of such previously-stolen information offered for sale on various social media and online platforms;

c. conspirators create a counterfeit check (as noted above, either utilizing check-printing software, or through physical alteration of pre-existing checks) that purports to have been drafted by the victim on victim's actual checking account, and made payable to the complicit third party;

d. conspirators, using the complicit third party's ATM card and accompanying PIN, deposit the counterfeit check at an ATM machine and then—following the bank's acceptance of that counterfeit check, and crediting of the complicit third party's account—withdraw the cash that the bank makes available.

4. It was further part of the conspiracy that conspirators, some of whom were employed by financial institutions, utilized that insider access to those financial institutions' systems and records to create bank accounts for other conspirators at the financial institutions, and to subsequently facilitate the deposit and negotiation of counterfeit and fraudulent checks within those bank accounts.

5. It was further part of the conspiracy that conspirators created or obtained fictitious identification documents, such as driver's licenses, that utilized the personal identifying

information of other individuals but the identity photographs of the conspirators. These fictitious means of identification constituted "counterfeit access devices" as that term is defined at 18 U.S.C. § 1029(e)(2).

6. It was further part of the conspiracy that conspirators utilized the credit cards, debit cards, and personal identifying information of other individuals that the conspirators obtained through their mail thefts and misappropriations to access the bank accounts of the legitimate account holders and withdraw funds from those accounts via ATM and Interactive Teller Machine (ITM) transactions. The misappropriated credit and debit cards possessed and utilized by the conspirators constituted "access devices" and "unauthorized access devices" as those terms are defined at 18 U.S.C. §§ 1029(e)(1) and (3), respectively.

7. Further, conspirators utilized the personal identifying information of other individuals, obtained through the theft of United States mail and other unlawful means, to apply for loans in the names of those individuals from financial institutions at which the victims maintained accounts. The conspirators would then utilize the victims' access devices—likewise obtained through the theft of United States mail and other unlawful means—to gain access to the victims' accounts and withdraw the loan proceeds.

8. Throughout the course of the conspiracy, the conspirators possessed and utilized the names, dates of birth, Social Security numbers, addresses, and banking information of other individuals in the form of stolen checks, stolen credit and debit cards, and stolen mail containing personally identifiable information. These purloined items constituted means of identification of those other individuals, as that term is defined at Title 18, United States Code, Section 1028(d)(7). The conspirators also possessed and utilized the names, ATM cards, and PINs of the above-described complicit third parties, each of which independently constituted a means of identification

of those persons, as that term is defined at Title 18, United States Code, Section 1028(d)(7).

9. The banking institutions targeted by the conspirators throughout the course of the conspiracy were each a "financial institution" at that term is defined at 18 U.S.C. § 20, to include the Virginia-based Virginia Credit Union (VACU).

Execution of the Scheme and Artifice to Defraud

To execute the above-described scheme and artifice to defraud, ELLERBE and his co-conspirators committed or caused the commission of the following acts, among others, in the Eastern District of Virginia and elsewhere:

10. On or about November 15, 2023, ELLERBE and another conspirator utilized the misappropriated bank account number and Social Security number of Victim 1 to access a Virginia Credit Union ("VACU") account belonging to Victim 1. ELLERBE and his co-conspirator accessed Victim 1's account from the exterior ITM of VACU's Scott's Addition (Richmond) branch location, and withdrew $15,000 in United States currency from one of Victim 1's accounts.

11. On or about November 15, 2023, ELLERBE and another conspirator utilized the misappropriated bank account number and Social Security number of Victim 1 to access a Virginia Credit Union ("VACU") account belonging to Victim 1. ELLERBE and his co-conspirator accessed Victim 1's account from the exterior ITM of VACU's Scott's Addition (Richmond) branch location, and withdrew $1,000 in United States currency from one of Victim 1's accounts.

12. On or about November 15, 2023, ELLERBE and another conspirator utilized the misappropriated bank account number and Social Security number of Victim 1 to access a Virginia Credit Union ("VACU") account belonging to Victim 1. ELLERBE and his co-conspirator accessed Victim 1's account from the exterior ITM of VACU's Scott's Addition (Richmond) branch location, and withdrew $6,000 in United States currency from one of Victim 1's accounts.

13. On or about November 15, 2023, ELLERBE and another conspirator utilized the misappropriated bank account number and Social Security number of Victim 1 to access a Virginia Credit Union ("VACU") account belonging to Victim 1. ELLERBE and his co-conspirator accessed Victim 1's account from the exterior ITM of VACU's Church Hill (Richmond) branch location, and withdrew $25,000 in United States currency from one of Victim 1's accounts.

14. On or about November 15, 2023, ELLERBE and another conspirator utilized the misappropriated bank account number and Social Security number of Victim 1 to access a Virginia Credit Union ("VACU") account belonging to Victim 1. ELLERBE and his co-conspirator accessed Victim 1's account from the exterior ITM of VACU's Carytown (Richmond) branch location, and withdrew $37,000 in United States currency from V one of Victim 1's accounts.

15. On or about November 15, 2023, ELLERBE and another conspirator utilized the misappropriated bank account number and Social Security number of Victim 1 to access a Virginia Credit Union ("VACU") account belonging to Victim 1. ELLERBE and his co-conspirator accessed Victim 1's account from the exterior ITM of VACU's Scott's Addition branch location, and withdrew $1,000 in United States currency from one of Victim 1's accounts.

16. On or about September 6, 2023, ELLERBE deposited a fraudulent check drafted on the bank account of Victim 2 for the face amount of $7,705.60 and made payable to ELLERBE, into a bank account opened in ELLERBE's own name by another conspirator, knowing at all times that the check in question was fraudulent, for the purpose of subsequently negotiating that fraudulent check and obtaining funds belonging to Victim 2.

17. On or about October 5, 2023, conspirators utilized an unauthorized access device belonging to Victim 3 to withdraw $20,000 from Victim 3's bank account—funds which the financial institution in question had credited to Victim 3's account as a result of a fraudulent loan

application submitted by the conspirators in Victim 3's name.

* * * *

18. ELLERBE and his co-conspirator were confronted by law enforcement officers shortly after completing their final transaction on November 15, 2023. Officers took Ellerbe into custody after a brief pursuit. At the time of his arrest, ELLERBE possessed numerous items stolen from the United States mail, to include: 83 stolen checks, $59,940 in United States currency, nine (9) stolen credit or debit cards, and six (6) stolen United States Savings Bonds. ELLERBE also possessed a Glock 21 handgun on his person.

19. A subsequent search of a vehicle rented by ELLERBE (and utilized by ELLERBE) during the course of the conspiracy also located additional items related to the above-described conspiracy to defraud, to include: a VACU debit card in the name of another individual; a counterfeit Washington D.C. Driver's License bearing the name and personal identifying information of that same individual (but depicting ELLERBE's image); and additional materials stolen from the United States mail.

(In violation of Title 18, United States Code, Section 1349).

COUNT TWO
(Possession of Stolen Mail)

THE UNITED STATES ATTORNEY FURTHER CHARGES THAT:

20. On or about November 15, 2023, in the Eastern District of Virginia, the defendant, OLDEN ELLERBE, III, did unlawfully have in his possession a check belonging to Victim 4 which had been stolen, taken, embezzled and abstracted from a mail receptacle which was an authorized depository for mail matter, knowing the said item to have been stolen, taken, embezzled and abstracted from an authorized depository for mail matter.

(In violation of Title 18, United States Code, Section 1708(a)(1)).

FORFEITURE ALLEGATION

21. Pursuant to Rule 32.2 of the Federal Rules of Criminal Procedure, the defendant is notified that as to Count 1 of this Criminal Information, the defendant, upon conviction of the offense, shall forfeit to the United States any property which constitutes, or is derived from, proceeds he obtained directly or indirectly, as the result of such offense.

22. The defendant is further notified that upon conviction of the offense in Count Two of this Criminal Information, he shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to the offense.

23. If the property subject to forfeiture cannot be located, the United States will seek an order forfeiting substitute assets.

(All in accordance with Title 18, United States Code, Sections 982(a)(2)(A), and(981(a)(1)(C), as incorporated by 28 U.S.C. § 2461(c) and Title 21, United States Code, Section 853(p)).

JESSICA D. ABER
UNITED STATES ATTORNEY

By: _____
Thomas A. Garnett
Robert S. Day
Assistant United States Attorneys